

DASAR KESELAMATAN ICT

JABATAN PERTAHANAN AWAM MALAYSIA
(JPAM)

Versi 1.0
Tahun 2009

Isi Kandungan

Mukasurat

Bahagian 1: Pendahuluan	1
Bahagian 2: Pernyataan Dasar Keselamatan ICT JPAM	4
Bahagian 3: Glosari	15
Bahagian 4: Pengurusan Penilaian Risiko Keselamatan ICT	17
Bahagian 5: Pelaksanaan Dasar Keselamatan ICT JPAM.....	19
Bahagian 6: Pengurusan Keselamatan ICT.....	21
Bahagian 7: Pengurusan Aset ICT.....	28
Bahagian 8: Keselamatan Sumber Manusia.....	30
Bahagian 9: Keselamatan Fizikal dan Persekitaran.....	33
Bahagian 10: Pengurusan Operasi dan Komunikasi.....	41
Bahagian 11: Kawalan Capaian.....	48
Bahagian 12: Perolehan, Pembangunan dan Penyelenggaraan Sistem Maklumat..	54
Bahagian 13: Pengurusan Pengendalian Insiden Keselamatan.....	58
Bahagian 14: Pengurusan Kesenambungan.....	62
Bahagian 15: Pematuhan.....	64

Bahagian 1: Pendahuluan

1.1 Pengenalan

Jabatan Pertahanan Awam Malaysia (JPAM) sedar akan tanggungjawab untuk memastikan keselamatan aset teknologi maklumat dan komunikasi (*information and communication technology*), ringkasnya ICT, yang dimiliki atau di bawah jagaan dan kawalannya. Ini termasuk semua data, peralatan, rangkaian dan kemudahan ICT. Tanggungjawab ini juga harus dipikul oleh ahli pentadbiran JPAM, pegawai dan kakitangan atau sesiapa sahaja yang mengakses dan yang menggunakan aset ICT Kerajaan.

1.2 Rasional

Tujuan utama keselamatan ICT adalah untuk menjamin kesinambungan urusan JPAM dengan meminimumkan kesan insiden keselamatan. Aset ICT perlu dilindungi kerana ia merupakan pelaburan besar JPAM bagi meningkatkan kecekapan dan keberkesanan sistem penyampaian.

Begitu juga dengan maklumat yang tersimpan di dalam ICT. Ia amat berharga kerana banyak sumber yang telah digunakan untuk menghasilkannya dan sukar untuk dijana semula dalam jangka masa yang singkat. Tambahan pula terdapat maklumat yang diproses oleh sistem ICT adalah sensitif dan terperingkat.

Pendedahan tanpa kebenaran atau pembocoran rahsia boleh memudaratkan kepentingan Negara. Sebarang penggunaan aset ICT selain daripada maksud dan tujuan yang telah ditetapkan, adalah merupakan satu penyalahgunaan sumber JPAM.

Ancaman ke atas keselamatan ICT boleh memberi kesan ke atas semua pihak termasuklah aset yang dikendalikan. Ancaman tersebut termasuklah perbuatan jenayah terhadap kakitangan, kecurian, penipuan, vandalisme, kebakaran, bencana alam, ralat atau kegagalan teknikal serta kerosakan yang tidak disengajakan.

Ancaman dari serangan siber dan aktiviti kod-kod jahat melalui Internet semakin meningkat dan mampu menjejaskan sistem penyampaian dan infrastruktur kritikal JPAM.

Memandangkan pentingnya aset ICT dilindungi, maka satu Dasar Keselamatan ICT JPAM adalah perlu diwujudkan.

1.3 Struktur Dokumen

Dokumen ini terbahagi kepada lima belas (15) bahagian iaitu:

Bahagian 1 : Pendahuluan

Bahagian ini menerangkan tujuan, rasional dan struktur kandungan dokumen Dasar Keselamatan ICT JPAM.

Bahagian 2 : Pernyataan Dasar Keselamatan ICT JPAM

Bahagian ini menerangkan Pernyataan Dasar, Objektif Dasar Keselamatan dan Prinsip-prinsip Dasar Keselamatan ICT JPAM.

Bahagian 3 : Glosari

Bahagian ini menerangkan istilah-istilah utama yang digunakan di dalam dokumen ini.

Bahagian 4 : Pengurusan Pelaksanaan Penilaian Risiko

Bahagian ini menerangkan keperluan melaksanakan penilaian risiko bagi mengenal pasti aset, ancaman serta kawalan yang boleh digunakan.

Bahagian 5 : Pelaksanaan Dasar Keselamatan ICT JPAM

Bahagian ini menerangkan hala tuju dan peraturan bagi mengguna dan seterusnya melindungi aset ICT JPAM.

Bahagian 6 : Pengurusan Keselamatan ICT

Bahagian ini menerangkan rangka kerja menguruskan keselamatan ICT JPAM.

Bahagian 7 : Pengurusan Aset ICT

Bahagian ini menerangkan keperluan mengenal pasti, mengelaskan dan mengendalikan aset ICT.

Bahagian 8 : Keselamatan Sumber Manusia

Bahagian ini menerangkan keperluan setiap individu termasuk pegawai dan kakitangan JPAM, **pembekal, pakar runding dan pihak-pihak lain** yang berkepentingan memahami tanggungjawab dan peranan mereka dalam keselamatan ICT.

Bahagian 9 : Keselamatan Fizikal dan Persekitaran

Bahagian ini menerangkan keperluan menyediakan perlindungan dan kawalan dari capaian yang tidak dibenarkan, kecuaihan, kerosakan dan gangguan terhadap persekitaran premis dan maklumat.

Bahagian 10 : Pengurusan Operasi dan Komunikasi

Bahagian ini menerangkan keperluan memastikan kemudahan pemrosesan maklumat dan komunikasi adalah sempurna dan selamat.

Bahagian 11 : Kawalan Capaian

Bahagian ini menerangkan keperluan menyediakan kawalan capaian ke atas maklumat.

Bahagian 12 : Perolehan, Pembangunan dan Penyelenggaraan Sistem Maklumat

Bahagian ini menerangkan keperluan memastikan aspek keselamatan semasa perancangan, rekabentuk dan perolehan di dalam semua sistem maklumat termasuk sistem pengoperasian, infrastruktur, sistem aplikasi pakej dan perkhidmatan.

Bahagian 13 : Pengurusan Pengendalian Insiden Keselamatan Maklumat

Bahagian ini menerangkan keperluan mengendalikan insiden dengan cepat, tepat dan berkesan.

Bahagian 14 : Pengurusan Kesenambungan Perkhidmatan

Bahagian ini menerangkan keperluan menjamin operasi perkhidmatan sistem penyampaian adalah sentiasa berterusan.

Bahagian 15 : Pematuhan

Bahagian ini menerangkan keperluan menghindar pelanggaran undang-undang jenayah dan sivil, peraturan atau ikatan kontrak dan sebarang keperluan keselamatan lain.

1.4 Sasaran

Dokumen ini disasarkan kepada setiap pegawai dan kakitangan JPAM, **pembekal, pakar runding dan pihak-pihak lain** yang mempunyai kepentingan di dalam mengendalikan maklumat JPAM.

Bahagian 2 : Penyataan Dasar Keselamatan ICT JPAM

Keselamatan ditakrifkan sebagai keadaan yang bebas daripada ancaman dan risiko yang tidak boleh diterima. Keselamatan adalah suatu proses yang berterusan. Ia melibatkan aktiviti berkala yang mesti dilakukan dari semasa ke semasa untuk menjamin keselamatan kerana ancaman dan kelemahan sentiasa berubah.

Keselamatan ICT adalah bermaksud keadaan di mana segala urusan menyediakan dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan. Keselamatan ICT berkait rapat dengan perlindungan aset ICT. Terdapat empat (4) komponen asas keselamatan ICT, iaitu

- (a) Melindungi maklumat rahsia rasmi dan maklumat rasmi JPAM dari capaian tanpa kuasa yang sah;
- (b) Menjamin setiap maklumat adalah tepat dan sempurna;
- (c) Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan
- (d) Memastikan akses kepada hanya pengguna-pengguna yang sah atau penerimaan maklumat dari sumber yang sah.

Dasar Keselamatan ICT JPAM merangkumi perlindungan ke atas semua bentuk maklumat elektronik bertujuan untuk menjamin keselamatan maklumat tersebut dan kebolehsediaan kepada semua pengguna yang dibenarkan. Ciri-ciri utama keselamatan maklumat adalah seperti berikut:

- (a) Kerahsiaan – Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran;
 - (b) Integriti – Data dan maklumat hendaklah tepat, lengkap dan kemas kini. Ia hanya boleh diubah dengan cara yang dibenarkan;
 - (c) Tidak Boleh Disangkal – Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal;
-

- (d) Kesahihan – Data dan maklumat hendaklah dijamin kesahihannya; dan
- (e) Kebolehsediaan – Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

Selain itu, langkah-langkah ke arah keselamatan ICT hendaklah bersandarkan kepada penilaian yang bersesuaian dengan perubahan semasa terhadap kelemahan semula jadi aset ICT; ancaman yang wujud akibat daripada kelemahan tersebut; risiko yang mungkin timbul; dan langkah-langkah pencegahan sesuai yang boleh diambil untuk menangani risiko berkenaan.

2.1 Prinsip-Prinsip Dasar Keselamatan ICT JPAM

Prinsip-prinsip yang menjadi asas kepada Dasar Keselamatan ICT JPAM adalah seperti berikut;

- (a) Akses atas dasar “perlu mengetahui”;
- (b) Hak akses minimum;
- (c) Akauntabiliti;
- (d) Pengasingan;
- (e) Pengauditan;
- (f) Pematuhan;
- (g) Pemulihan; dan
- (h) Saling bergantung.

2.1.1 Akses Atas Dasar Perlu Mengetahui

Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar “perlu mengetahui” sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atas fungsi pengguna memerlukan maklumat tersebut. Pertimbangan akses di bawah prinsip ini adalah berasaskan

kepada klasifikasi maklumat dan tapisan keselamatan pengguna seperti berikut:

(a) Klasifikasi Maklumat

Keselamatan ICT JPAM hendaklah mematuhi “Arahan Keselamatan” perenggan 53, muka surat 15, di mana maklumat dikategorikan kepada Rahsia Besar, Rahsia, Sulit dan Terhad. Data, bahan atau maklumat rasmi yang sensitif atau bersifat terperingkat perlu dilindungi dari pendedahan, dimanipulasi atau diubah semasa dalam penghantaran. Penggunaan kod dan tandatangan digital mesti dipertimbangkan bagi melindungi data dikirim secara elektronik. Dasar kawalan akses ke atas aplikasi atau sistem juga hendaklah mengikuti klasifikasi maklumat yang sama, iaitu sama ada rahsia besar, rahsia, sulit atau terhad; dan

(b) Tapisan Keselamatan Pengguna

Dasar Keselamatan ICT JPAM adalah mematuhi prinsip bahawa pengguna boleh diberi kebenaran mengakses kategori maklumat tertentu setelah siasatan latar belakang menunjukkan tiada sebab atau faktor untuk menghalang pengguna daripada berbuat demikian.

2.1.2 Hak Akses Minimum

Hak akses kepada pengguna hanya diberi pada tahap set yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan khas adalah diperlukan untuk membolehkan pengguna mewujudkan, menyimpan, mengemaskini, mengubah atau membatalkan sesuatu data atau maklumat.

2.1.3 Akauntabiliti

Semua pengguna adalah dipertanggungjawabkan ke atas semua tindakannya terhadap aset ICT. Tanggungjawab ini perlu dinyatakan dengan jelas sesuai dengan tahap sensitiviti sesuatu sumber ICT. Untuk menentukan tanggungjawab ini dipatuhi, sistem ICT hendaklah

mampu menyokong kemudahan mengesan atau mengesah bahawa pengguna sistem maklumat boleh dipertanggungjawabkan atas tindakan mereka.

Akauntabiliti atau tanggungjawab pengguna termasuklah:

- (a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
- (b) Memeriksa maklumat dan menentukan ianya tepat dan lengkap dari semasa ke semasa;
- (c) Menentukan maklumat sedia untuk digunakan;
- (d) Menjaga kerahsiaan kata laluan;
- (e) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;
- (f) Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan
- (g) Menjaga kerahsiaan langkah-langkah keselamatan ICT daripada diketahui umum.

2.1.4 Pengasingan

- (a) Prinsip pengasingan bermaksud bahawa semua tugas-tugas mewujudkan, memadam, mengemaskini, mengubah dan mengesahkan data diasingkan. Ia bertujuan untuk mengelak akses yang tidak dibenarkan dan melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat, dimanipulasi dan seterusnya, mengekalkan integriti dan kebolehsediaan; dan
 - (b) Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian. Ia bertujuan untuk mengasingkan akses kepada domain kedua-dua kumpulan tersebut seperti akses kepada fail data, fail program,
-

kemudahan sistem dan komunikasi, manakala pemisahan perubahan pada konfigurasi dan keperluan sistem.

2.1.5 Pada tahap minimum, semua sistem ICT perlu mengekalkan persekitaran operasi yang berasingan seperti berikut:

- (a) Persekitaran pembangunan di mana sesuatu aplikasi dalam proses pembangunan;
- (b) Persekitaran penerimaan iaitu peringkat di mana sesuatu aplikasi diuji dan dibuat penerimaan pengguna; dan
- (c) Persekitaran sebenar di mana aplikasi sedia untuk beroperasi.

2.1.6 Pengauditan

- (a) Pengauditan adalah tindakan untuk mengenal pasti insiden berkaitan keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan. Dengan itu, aset ICT seperti komputer, pelayan, *router*, *firewall*, dan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau *audit trail*. Pentingnya *audit trail* ini menjadi semakin ketara apabila wujud keperluan untuk mengenal pasti punca masalah atau ancaman kepada keselamatan ICT. Oleh itu, rekod audit hendaklah dilindungi dan tersedia untuk penilaian atau tindakan sertamerta;
 - (b) Pengauditan juga perlu dibuat ke atas rekod-rekod manual seperti dokumen operasi, nota serah tugas, kelulusan keluar pejabat, memorandum, borang kebenaran, surat kuasa, senarai inventori dan kemudahan akses log. Ini adalah kerana dalam kes-kes tertentu, dokumen ini diperlukan untuk menyokong *audit trail* sistem komputer; dan
 - (c) Keseluruhannya, sistem pengauditan ini adalah penting dalam menjamin akauntabiliti. Antara lain, sistem ini dapat dirujuk bagi menentukan perkara-perkara berikut:
-

- i. Mengesan pematuhan atau pelanggaran keselamatan;
- ii. Menyediakan catatan peristiwa mengikut urutan masa yang boleh digunakan untuk mengesan punca berlakunya pelanggaran keselamatan; dan
- iii. Menyediakan bahan bukti bagi menentukan sama ada berlakunya pelanggaran keselamatan.

2.1.7 Pematuhan

Pematuhan adalah merupakan prinsip penting dalam menghindar dan mengesan sebarang pelanggaran Dasar. Pematuhan kepada Dasar Keselamatan ICT JPAM boleh dicapai melalui tindakan berikut:

- (a) Mewujud proses yang sistematik khususnya dalam menjamin keselamatan ICT untuk memantau dan menilai tahap pematuhan langkah-langkah keselamatan yang telah dikuatkuasakan;
- (b) Merumus pelan pematuhan untuk menangani sebarang kelemahan atau kekurangan langkah-langkah keselamatan ICT yang dikenalpasti;
- (c) Melaksana program pemantauan keselamatan secara berterusan untuk memastikan standard, prosedur dan garis panduan keselamatan dipatuhi; dan
- (d) Menguatkuasa amalan melapor sebarang peristiwa yang mengancam keselamatan ICT dan seterusnya mengambil tindakan pembedahan.

2.1.8 Pemulihan

Pemulihan sistem amat perlu untuk memastikan kebolehsediaan dan kebolehcapaian. Objektif utama adalah untuk meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan. Antara lain, pemulihan boleh dilakukan melalui tindakan-tindakan berikut:

- (a) Merumus dan menguji Pelan Pemulihan Bencana – (*Disaster Recovery Plan*); dan
-

- (b) Mengamalkan langkah-langkah membuat salinan data dan lain-lain amalan baik dalam penggunaan ICT seperti menghapuskan virus, langkah-langkah pencegahan kebakaran dan amalan *clear desk*.

2.1.9 Saling Bergantung

Langkah-langkah keselamatan ICT yang berkesan memerlukan pematuhan kepada semua prinsip-prinsip di atas. Setiap prinsip adalah saling lengkap-melengkapi antara satu dengan lain. Dengan itu, tindakan mempelbagaikan pendekatan dalam menyusun dan mencorak sebanyak mungkin mekanisme keselamatan, dapat menjamin keselamatan yang maksimum. Prinsip saling bergantung meliputi beberapa peringkat di mana di tahap minimum, mengandungi langkah-langkah berikut;

- (a) Sambungan kepada internet - Semua komunikasi antara sistem ICT dengan sistem luar hendaklah melalui mekanisme pusat untuk mengurus, menguatkuasa dan mengawas sebarang bahaya keselamatan. Melalui sistem ini, semua trafik dalaman hendaklah melalui *gateway firewall* yang diurus secara berpusat. Semua trafik dari luar ke dalam hendaklah juga melalui laluan ini atau melalui kumpulan modem yang dikawal secara berpusat. Dengan itu, penggunaan modem dalaman tidak dibenarkan;
 - (b) *Backbone* Rangkaian – *Backbone* rangkaian akan hanya mengendalikan trafik yang telah dikod untuk meminimumkan intipan;
 - (c) Rangkaian JPAM – Semua rangkaian JPAM akan dihubungkan ke *backbone* melalui *firewall* yang mana akan pula mengkod semua trafik di antara rangkaian JPAM dengan rangkaian di peringkat yang seterusnya atau pusat data; dan
 - (d) Pelayan JPAM – Semua data dan maklumat yang kritikal atau sensitif akan hanya disimpan di pelayan JPAM atau di pelayan yang diurus secara pusat. Ini akan meminimumkan pendedahan, pengubahan atau kecurian. Semua data dan maklumat sensitif akan dikodkan.
-

2.2 Objektif Dasar Keselamatan ICT JPAM

- 2.2.1 Objektif utama Dasar Keselamatan ICT JPAM ialah seperti berikut;
- (a) Memastikan kelancaran operasi JPAM dan meminimumkan kerosakan atau kemusnahan;
 - (b) Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat daripada kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi; dan
 - (c) Mencegah salah guna, kecuaiian atau kecurian aset ICT.
- 2.2.2 Dasar Keselamatan ICT JPAM ini juga bertujuan memudahkan perkongsian maklumat sesuai dengan keperluan operasi JPAM. Ini hanya boleh dicapai dengan memastikan semua aset ICT dilindungi.

2.3 Skop Dasar Keselamatan ICT JPAM

- 2.3.1 Sistem ICT JPAM terdiri daripada perkakasan, perisian, manusia, perkhidmatan dan data atau maklumat. Sistem ini adalah aset yang amat berharga di mana pengguna (jabatan-jabatan Kerajaan, pihak swasta, warganegara dan bukan warganegara yang bermastautin) bergantung untuk menjalankan urusan rasmi dengan lancar. Dengan itu, Dasar Keselamatan ICT JPAM menetapkan keperluan-keperluan asas berikut:
- (a) Data dan maklumat hendaklah boleh diakses secara berterusan dengan cepat, tepat, mudah dan berintegriti dengan cara yang boleh dipercayai. Ini adalah amat perlu bagi membolehkan keputusan dan penyampaian perkhidmatan dilakukan dengan berkesan dan berkualiti; dan
 - (b) Semua data dan maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi
-

memastikan kesempurnaan dan ketepatan maklumat serta untuk melindungi kepentingan JPAM, perkhidmatan dan masyarakat.

- 2.3.2 Memandangkan sistem ICT sangat kompleks dan terdedah kepada ancaman dan risiko, adalah tidak mudah untuk memenuhi keperluan ini. Sistem ICT dan komponennya saling berhubungan dan bergantung antara satu dengan lain kerap kali mewujudkan pelbagai risiko. Sesetengah risiko hanya menjadi kenyataan setelah masa berlalu manakala sesetengahnya timbul apabila berlaku perubahan. Walau bagaimanapun risiko seperti ini hendaklah dikenal pasti dan ditangani sewajarnya.
- 2.3.3 Bagi menangani risiko ini dari semasa ke semasa, Dasar Keselamatan ICT JPAM akan diperjelaskan melalui pengeluaran Standard Keselamatan ICT yang mengandungi garis panduan serta langkah-langkah keselamatan ICT. Kegunaan kesemua dokumen ini secara bersepadu adalah disarankan. Ini adalah kerana pembentukan dasar, standard, garis panduan dan langkah-langkah keselamatan ini diorientasi untuk melindungi kerahsiaan data, maklumat dan sebarang kesimpulan yang boleh dibuat daripadanya.
- 2.3.4 Bagi menentukan Sistem ICT ini terjamin keselamatannya sepanjang masa, Dasar Keselamatan ICT JPAM ini merangkumi perlindungan semua bentuk maklumat Kerajaan yang dimasukkan, diwujudkan, dimusnah, disimpan, dijana, dicetak, diakses, diedar dalam penghantaran, dan yang dibuat salinan keselamatan ke dalam semua aset ICT. Ini akan dilakukan melalui penubuhan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua perkara-perkara berikut:
- (a) Perkakasan – Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan jabatan. Contoh: komputer, pelayan, peralatan komunikasi dan sebagainya.
 - (b) Perisian – Program, prosedur atau peraturan yang ditulis dan dokumentasi yang berkaitan dengan sistem pengoperasian komputer yang disimpan di dalam sistem ICT. Contoh perisian aplikasi atau perisian sistem seperti sistem pengoperasian, sistem pangkalan data, perisian system rangkaian, atau
-

aplikasi pejabat yang menyediakan kemudahan pemrosesan maklumat kepada jabatan;

- (c) Perkhidmatan – Perkhidmatan atau sistem yang menyokong aset lain untuk melaksanakan fungsi-fungsinya. Contoh:
 - i. Perkhidmatan rangkaian seperti LAN, WAN dan lain-lain.
 - ii. Sistem halangan akses seperti sistem kad akses.
 - iii. Perkhidmatan sokongan seperti kemudahan elektrik, penghawa dingin, sistem pencegahan kebakaran dan lain-lain.
- (d) Data atau Maklumat – Koleksi fakta-fakta dalam bentuk kertas atau mesej elektronik, yang mengandungi maklumat-maklumat untuk digunakan bagi mencapai misi dan objektif jabatan. Contoh: Sistem dokumentasi, prosedur operasi, rekod-rekod jabatan, profil-profil pelanggan, pangkalan data dan fail-fail data, maklumat-maklumat arkib dan lain-lain.
- (e) Manusia – Individu yang mempunyai pengetahuan dan kemahiran untuk melaksanakan skop kerja harian jabatan bagi mencapai misi dan objektif jabatan. Individu berkenaan merupakan aset berdasarkan kepada tugas-tugas dan fungsi yang dilaksanakan.

2.3.5 Setiap perkara di atas perlu diberi perlindungan rapi. Sebarang kebocoran rahsia atau kelemahan perlindungan adalah dianggap sebagai pelanggaran langkah- langkah keselamatan.

2.3.6 Di samping itu, Dasar Keselamatan ICT JPAM ini juga adalah saling lengkap-melengkapi dan perlu dilaksanakan secara konsisten dengan undang-undang dan peraturan yang sedia ada.

2.4 Pindaan dan Kemas kini

Dasar Keselamatan ICT JPAM adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Dasar ini hendaklah dibaca bersama dokumen-dokumen mengenai standard, garis panduan, prosedur dan langkah keselamatan ICT Kerajaan yang dikeluarkan dari semasa ke semasa.

2.5 Maklumat Lanjut

Sebarang pertanyaan mengenai kandungan dokumen ini atau permohonan untuk keterangan lanjut, boleh ditujukan kepada:

Unit Teknologi Maklumat

Jabatan Pertahanan Awam Malaysia
Kementerian Dalam Negeri
Jalan Padang Tembak
50556 Kuala Lumpur

Telefon : 03-26871300, 03-26871421
Faks : 03-26943448
E-mel : jpamcert@civildefence.gov.my

Rangka Dasar Keselamatan ICT JPAM ini juga boleh diakses di laman web JPAM (<http://www.civildefence.gov.my>)

Bahagian 3: Glosari

(a) Risiko

Bermaksud kemungkinan yang boleh menyebabkan bahaya, kerosakan dan kerugian.

(b) Penilaian Risiko

Bermaksud penilaian ke atas kemungkinan berlakunya bahaya, kerosakan atau kehilangan aset.

(c) Ancaman

Bermaksud apa sahaja kejadian yang berpotensi atau tindakan yang boleh menyebabkan berlaku kemusnahan atau musibah

(d) Vulnerability

Bermaksud sebarang kelemahan pada aset atau sekumpulan aset yang boleh dieksploitasi oleh ancaman.

(e) Insiden Keselamatan

Bermaksud musibah (*adverse event*) yang berlaku ke atas sistem maklumat.

(f) Aset ICT

Bermaksud semua yang mempunyai nilai kepada organisasi merangkumi perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.

(g) Penyulitan

Bermaksud menjadikan teks biasa (*plain text*) kepada kod yang tidak dapat difahami dan kod yang tidak difahami ini akan menjadi versi teks *cipher*. Bagi mendapatkan semula teks biasa tersebut, proses penyahsulitan digunakan.

(h) Clear Desk

Bermaksud tidak meninggalkan sebarang dokumen yang sensitif di atas meja.

(i) ***Clear Screen***

Bermaksud tidak memaparkan sebarang maklumat sensitif apabila komputer berkenaan ditinggalkan.

(j) ***Mobile Code***

Bermaksud kod perisian yang dipindahkan dari satu komputer kepada komputer lain dan melaksanakan secara automatik fungsi-fungsi tertentu dengan sedikit atau tanpa interaksi dari pengguna.

(k) **Kriptografi**

Bermaksud adalah satu sains penulisan kod rahsia yang membolehkan penghantaran dan storan data dalam bentuk yang hanya difahami oleh pihak yang tertentu sahaja.

(l) ***Business Resumption Plan (BRP)***

Bermaksud pelan yang berupaya untuk meneruskan operasi jika berlaku gangguan perkhidmatan. Dalam situasi pelan sukar dilaksanakan sepenuhnya, maka pelan ini seboleh-bolehnya dapat melaksanakan fungsi-fungsi bagi operasi teras.

Bahagian 4: Pengurusan Penilaian Risiko Keselamatan ICT

JPAM sentiasa mengambil kira kewujudan risiko ke atas aset ICT akibat dari ancaman dan kerentanan yang semakin meningkat hari ini. Justeru, jabatan perlu mengambil langkah-langkah proaktif dan bersesuaian untuk menilai tahap risiko aset ICT supaya pendekatan dan keputusan yang paling berkesan dikenalpasti bagi menyediakan perlindungan dan kawalan ke atas aset ICT.

Penilaian risiko keselamatan aset ICT bertujuan membolehkan jabatan mengukur, menganalisis tahap risiko aset ICT dan seterusnya mengambil tindakan untuk merancang dan mengawal risiko.

4.1 Tanggungjawab Melaksanakan Penilaian Risiko Keselamatan ICT

Ketua Jabatan bertanggungjawab memastikan penilaian risiko keselamatan ICT dilaksanakan secara berkala dan berterusan. Keperluan melaksanakan penilaian risiko bergantung kepada perubahan ke atas persekitaran jabatan. Ketua Jabatan seterusnya hendaklah mengambil tindakan susulan dan/atau langkah-langkah bersesuaian untuk mengurangkan atau mengawal risiko keselamatan ICT berdasarkan penemuan penilaian risiko.

Ketua Jabatan hendaklah melaksanakan penilaian risiko mengikut peraturan atau prosedur yang ditetapkan oleh JPAM dari semasa ke semasa.

4.2 Skop Penilaian Risiko Keselamatan ICT

Penilaian risiko keselamatan ICT hendaklah dilaksanakan ke atas sistem maklumat di jabatan termasuklah aplikasi, perisian, pelayan, rangkaian dan/atau proses serta prosedur yang dikendalikan oleh jabatan. Penilaian risiko ini hendaklah juga dilaksanakan di permis yang menempatkan sumber-sumber teknologi maklumat termasuklah pusat data, bilik server, bilik media storan, kemudahan utiliti dan sistem-sistem sokongan lain.

4.3 Penentuan Tindakan Untuk Mengendalikan Risiko Keselamatan ICT

Setiap jabatan JPAM bertanggungjawab melaksanakan dan menguruskan risiko keselamatan ICT masing-masing. Melalui proses-proses yang dilaksanakan untuk

menilai risiko aset ICT Kerajaan, jabatan dapat mengenal pasti risiko-risiko yang wujud dan seterusnya mengenal pasti tindakan yang sewajarnya untuk menghadapi kemungkinan berlakunya risiko berkenaan.

Untuk mengenal pasti tindakan yang wajar diambil bagi menghadapi kemungkinan risiko terjadi termasuklah seperti berikut:

- (a) mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;
 - (b) menerima dan/atau bersedia berhadapan dengan risiko yang akan terjadi selagi ia memenuhi kriteria yang telah ditetapkan oleh pengurusan jabatan;
 - (c) mengelak dan/atau mencegah risiko dari terjadi dengan mengambil tindakan yang dapat mengelak dan/atau mencegah berlakunya risiko; dan
 - (d) memindahkan risiko ke pihak lain seperti pembekal, pakar runding dan pihak-pihak lain yang berkepentingan.
-

Bahagian 5: Pelaksanaan Dasar Keselamatan ICT JPAM

Penyataan Dasar:

JPAM hendaklah mewujudkan dan melaksanakan dasar-dasar yang jelas yang dapat menjamin perlindungan ke atas kerahsiaan, integriti dan kebolehsediaan maklumat dan seterusnya menjamin kesinambungan urusan dan perkhidmatan dengan meminimumkan kesan insiden keselamatan.

Objektif:

Untuk memberi hala tuju dan peraturan-peraturan bagi mengguna dan melindungi aset ICT selaras dengan keperluan undang-undang.

5. Pelaksanaan Dasar Keselamatan ICT JPAM

Seksyen ini bertujuan memastikan hala tuju pengurusan organisasi untuk melindungi aset ICT selaras dengan keperluan perundangan. Adalah menjadi tanggungjawab Ketua Jabatan ke atas pelaksanaan dasar dengan dibantu oleh jawatankuasa pengurusan keselamatan ICT yang terdiri daripada Ketua Pegawai Maklumat (CIO), Pegawai Keselamatan ICT (ICTSO) dan lain-lain pegawai yang dilantik. Dasar Keselamatan ICT JPAM hendaklah diterima pakai oleh pengurusan dan disebarkan kepada semua pegawai dan kakitangan JPAM.

5.1 Pemakaian Dasar Keselamatan ICT JPAM

Dasar Keselamatan ICT JPAM adalah terpakai kepada semua pengguna aset ICT termasuk pembekal, pakar runding dan pihak lain yang berurusan dengan JPAM dan tiada pengecualian diberikan.

5.2 Semakan dan Pindaan Dasar

Dasar Keselamatan ICT JPAM adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Prosedur penyelenggaraan Dasar Keselamatan ICT JPAM adalah termasuk yang berikut:

- (a) Menyemak dasar ini sekurang-kurangnya sekali setahun bagi mengenal pasti dan menentukan perubahan yang diperlukan; dan
 - (b) Mengemukakan cadangan perubahan secara bertulis kepada MAMPU, Jabatan Perdana Menteri.
-

Bahagian 6: Pengurusan Keselamatan ICT

Penyataan Dasar:

Satu rangka kerja pengurusan keselamatan ICT perlu diwujudkan supaya keselamatan ICT dilaksanakan dengan lebih sistematik, lancar dan berkesan.

Objektif:

Untuk mengurus keselamatan ICT di JPAM.

6. Pengurusan Keselamatan ICT

Adalah menjadi tanggungjawab Ketua Jabatan untuk:

- (a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT JPAM;
 - (b) Mewujud dan mengetuai jawatankuasa pengurusan keselamatan ICT organisasi;
 - (c) Memastikan semua pengguna ICT JPAM memahami dan mematuhi Dasar Keselamatan ICT JPAM;
 - (d) Memastikan semua keperluan keselamatan ICT JPAM iaitu, sumber kewangan, kakitangan dan perlindungan keselamatan adalah mencukupi;
 - (e) Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT JPAM; dan
-

- (f) Menandatangani Surat Akuan Pematuhan bagi mematuhi Dasar Keselamatan ICT JPAM.

6.1 Struktur Organisasi

Seksyen ini bertujuan memastikan struktur formal diwujudkan untuk menguruskan keselamatan ICT JPAM.

Jawatankuasa Pemandu ICT JPAM bertanggungjawab terhadap pengurusan keselamatan ICT JPAM.

Perkara yang perlu dipatuhi termasuk yang berikut:

- (a) Komitmen pengurusan atasan ke atas keselamatan ICT dilaksanakan dengan aktif dan telus;
- (b) Aktiviti pengurusan atasan ke atas keselamatan ICT diselaraskan oleh Ketua Bahagian dari semua peringkat organisasi berdasarkan peranan masing-masing;
- (c) Tanggungjawab yang jelas bagi semua pengguna ICT JPAM dalam pengurusan keselamatan ICT;
- (d) Keperluan untuk pengurusan kerahsiaan maklumat dikenal pasti, dilaksana dan dikaji secara berkala;
- (e) Memastikan jalinan perhubungan/komunikasi dengan pihak yang relevan dipelihara; dan
- (f) Memastikan kajian semula ke atas keselamatan maklumat dijalankan mengikut peraturan yang ditetapkan.

6.2 Pihak Luar/Asing

Seksyen ini bertujuan memastikan penggunaan maklumat dan kemudahan proses maklumat dan kemudahan proses maklumat oleh pihak luar/asing dikawal.

Perkara yang perlu dipatuhi termasuk yang berikut:

- (a) Mengetahui pasti risiko keselamatan maklumat dan kemudahan pemrosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian;
- (b) Mengetahui pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pengguna; dan
- (c) Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga.

Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai.

- i. Dasar Keselamatan ICT JPAM;
- ii. Tapisan Keselamatan;
- iii. Perakuan Akta Rahsia Rasmi 1972; dan
- iv. Hak Harta Intelek;

6.3 Jawatankuasa Pengurusan Keselamatan ICT

Seksyen ini bertujuan menerangkan peranan dan tanggungjawab ahli jawatankuasa pengurusan keselamatan ICT JPAM dan Jabatan di bawahnya.

- (a) Ketua Pegawai Maklumat (CIO)

Peranan dan tanggungjawab adalah termasuk seperti berikut:

- i. Membaca, memahami dan mematuhi Dasar Keselamatan ICT JPAM;
 - ii. Membantu Ketua Jabatan dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT;
 - iii. Menentukan keperluan keselamatan ICT;
 - iv. Membangun dan menyelaras pelaksanaan pelan latihan dan program kesedaran mengenai keselamatan ICT; dan
-

- v. Menandatangani Surat Akuan Pematuhan untuk mematuhi Dasar Keselamatan ICT JPAM.

(b) Pegawai Keselamatan ICT (ICTSO)

Peranan dan tanggungjawab adalah termasuk seperti berikut:

- i. Membaca, memahami dan mematuhi Dasar Keselamatan ICT JPAM;
 - ii. Mengurus keseluruhan program-program keselamatan ICT organisasi;
 - iii. Menguatkuasakan Dasar Keselamatan ICT JPAM;
 - iv. Memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT JPAM kepada semua pengguna;
 - v. Mewujudkan garis panduan dan prosedur selaras dengan keperluan Dasar keselamatan ICT JPAM;
 - vi. Melaksanakan pengurusan risiko;
 - vii. Melaksanakan pengauditan, mengkaji semula, merumus tindak balas pengurusan berdasarkan hasil penemuan dan menyediakan laporan mengenainya;
 - viii. Memberi amaran kepada semua pejabat negeri, daerah dan pusat latihan terhadap kemungkinan berlakunya ancaman keselamatan ICT seperti virus dan penggadam serta memberi khidmat nasihat dan bantuan teknikal bagi menyediakan langkah-langkah perlindungan yang bersesuaian;
 - ix. Melaporkan insiden keselamatan ICT kepada Pegawai Keselamatan ICT (ICTSO) JPAM dan kepada CERT JPAM atau/dan GCERT, MAMPU dan memaklukkannya kepada Ketua Jabatan, CIO dan Pengurusan ICT;
 - x. Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan
-

ICT dan memperakukan langkah-langkah baik pulih dengan segera;

- xi. Memberi perakuan tindakan tatatertib ke atas pengguna yang melanggar Dasar Keselamatan ICT JPAM;
- xii. Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT; dan
- xiii. Menandatangani Surat Akuan pematuhan untuk mematuhi Dasar Keselamatan ICT JPAM.

(c) Pengurusan ICT

Peranan dan tanggungjawab adalah termasuk seperti berikut:

- i. Membaca, memahami dan mematuhi Dasar Keselamatan ICT JPAM;
 - ii. Memastikan kajian semula dan pelaksanaan kawalan keselamatan ICT selaras dengan keperluan organisasi;
 - iii. Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO untuk tindakan;
 - iv. Memastikan penyampaian rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT organisasi dilaksanakan;
 - v. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai Pentadbir Sistem ICT yang berhenti, bertukar, bercuti panjang atau berlaku perubahan dalam bidang tugas; dan
 - vi. Menandatangani Surat Akuan Pematuhan untuk mematuhi Dasar Keselamatan ICT JPAM.
-

(d) Pentadbir Sistem ICT

Peranan dan tanggungjawab adalah termasuk seperti berikut:

- i. Membaca, memahami dan mematuhi Dasar Keselamatan ICT JPAM;
 - ii. Menjaga kerahsiaan kata laluan;
 - iii. Menjaga kerahsiaan konfigurasi aset ICT;
 - iv. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai semua pengguna ICT JPAM yang gantung kerja, berhenti, bersara, bertukar, bercuti panjang atau berlaku perubahan dalam bidang tugas;
 - v. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai pengguna luar dan pihak ketiga yang berhenti atau tamat projek;
 - vi. Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan;
 - vii. Memantau aktiviti capaian harian pengguna;
 - viii. Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran; membatalkan atau memberhentikanannya dengan serta-merta; dan memaklumkan kepada Pengurusan ICT untuk tindakan selanjutnya;
 - ix. Menyediakan laporan mengenai aktiviti capaian kepada pemilik maklumat berkenaan secara berkala;
 - x. Menyimpan dan menganalisis rekod jejak audit; dan
 - xi. Menandatangani Surat Akuan Pematuhan untuk mematuhi Dasar Keselamatan ICT JPAM.
-

(e) Pengguna Dalam

Peranan dan tanggungjawab adalah termasuk seperti berikut:

- i. Membaca, memahami dan mematuhi Dasar Keselamatan ICT JPAM;
- ii. Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya;
- iii. Melaksanakan langkah-langkah perlindungan seperti berikut:-
 - Menjaga kerahsiaan maklumat JPAM yang meliputi maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan;
 - Menjaga kerahsiaan kata laluan;
 - Memastikan maklumat berkaitan adalah tepat dan lengkap dari semasa ke semasa; dan
 - Menjaga kerahsiaan langkah-langkah keselamatan ICT daripada diketahui umum.
- iv. Menghadiri program-program kesedaran mengenai keselamatan ICT; dan
- v. Menandatangani Surat Akuan Pematuhan untuk mematuhi Dasar Keselamatan ICT JPAM.

Bahagian 7: Pengurusan Aset ICT

Penyataan Dasar:

Setiap aset ICT perlu dikenal pasti, dikelaskan, didokumenkan, diselenggarakan dan perlu dilupuskan apabila tiba masanya.

Objektif:

Untuk memberikan perlindungan keselamatan yang bersesuaian kepada semua aset ICT.

7. Pengurusan Aset ICT

Adalah menjadi tanggungjawab Ketua Jabatan untuk mengurus aset ICT di bawah kawalannya.

7.1 Tanggungjawab Ke Atas Aset ICT

Seksyen ini bertujuan memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing.

Tanggungjawab yang perlu dipatuhi adalah termasuk perkara-perkara berikut:

- (a) Memastikan semua aset dikenal pasti, dikelas, didokumen, diselenggara dan dilupuskan apabila tiba masanya di mana maklumat aset direkod dan dikemaskini dalam borang daftar harta modal dan inventori;

- (b) Memastikan semua aset mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; dan
- (c) Peraturan bagi pengendalian aset hendaklah dikenal pasti, didokumen dan dilaksanakan.

7.2 Pengelasan Maklumat

Seksyen ini bertujuan memastikan setiap maklumat diberi perlindungan yang bersesuaian berdasarkan tahap kerahsiaan.

Maklumat hendaklah dikelaskan berasaskan nilai, keperluan perundangan, tahap sensitiviti dan tahap kritikal kepada JPAM.

7.3 Pelabelan dan Pengendalian Maklumat

Pelabelan dan pengendalian maklumat seperti pewujudan, pengumpulan, pemprosesan, penyimpanan, penghantaran, penyampaian, penukaran dan pemusnahan hendaklah mengikut standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan.

Bahagian 8: Keselamatan Sumber Manusia

Penyataan Dasar:

Semua peranan dan tanggungjawab pegawai dan kakitangan JPAM, pembekal, pakar runding dan pihak-pihak lain hendaklah jelas dan didokumenkan mengikut Dasar Keselamatan ICT JPAM.

Objektif:

Untuk memastikan semua sumber manusia yang terlibat termasuk pegawai dan kakitangan JPAM, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan memahami tanggungjawab dan peranan mereka dalam keselamatan aset ICT.

8. Keselamatan Sumber Manusia

Ketua Jabatan adalah bertanggungjawab ke atas sumber manusia yang terlibat secara langsung atau tidak langsung dalam pengendalian aset ICT di bawah kawalannya.

8.1 Sebelum Berkhidmat

Seksyen ini bertujuan memastikan pegawai dan kakitangan JPAM, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan memahami tanggungjawab masing-masing ke atas keselamatan aset ICT bagi meminimumkan risiko seperti kesilapan, kecuaiian, kecurian, penipuan dan penyalahgunaan aset ICT.

Perkara yang mesti dipatuhi termasuk yang berikut:

- (a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pegawai dan kakitangan JPAM, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan ke atas keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan;
- (b) Menjalankan tapisan keselamatan untuk pegawai dan kakitangan JPAM, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan selaras dengan keperluan perkhidmatan; dan
- (c) Mematuhi terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuatkuasa berdasarkan perjanjian yang telah ditetapkan.

8.2 Dalam Perkhidmatan

Seksyen ini bertujuan memastikan pegawai dan kakitangan JPAM, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan sedar akan ancaman keselamatan maklumat, peranan dan tanggungjawab masing-masing untuk menyokong Dasar Keselamatan ICT jabatan dan meminimumkan risiko kesilapan, kecuaihan, kecurian, penipuan dan penyalahgunaan aset ICT.

Perkara yang perlu dipatuhi termasuk yang berikut:

- (a) Memastikan pegawai dan kakitangan JPAM, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan ditetapkan jabatan;
 - (b) Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pegawai dan kakitangan JPAM, sekiranya perlu diberi kepada pembekal, pakar runding dan pihak-pihak lain yang berkepentingan dari semasa ke semasa; dan
 - (c) Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas pegawai dan kakitangan JPAM, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan sekiranya berlaku pelanggaran dengan perundangan dan peraturan ditetapkan jabatan.
-

8.3 Bertukar Atau Tamat Perkhidmatan

Seksyen ini bertujuan memastikan pertukaran atau tamat perkhidmatan pegawai dan kakitangan JPAM, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan diurus dengan teratur.

Perkara yang perlu dipatuhi termasuk yang berikut:

- (a) Memastikan semua aset ICT dikembalikan kepada jabatan mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan
- (b) Membatalkan atau meminda semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan jabatan dan/atau terma perkhidmatan.

Bahagian 9: Keselamatan Fizikal dan Persekitaran

Penyataan Dasar:

Premis dan peralatan memproses maklumat yang kritikal dan sensitif hendaklah ditempatkan di kawasan yang selamat dan dilindungi dari sebarang ancaman fizikal dan persekitaran.

Objektif:

Untuk menghalang capaian yang tidak dibenarkan, kerosakan dan gangguan terhadap persekitaran premis, peralatan dan maklumat.

9. Keselamatan Fizikal dan Persekitaran

Adalah menjadi tanggungjawab Ketua Jabatan untuk mengesan, mencegah dan menghalang pencerobohan ke atas kawasan yang menempatkan peralatan, maklumat dan kemudahan pemrosesan maklumat yang boleh mengakibatkan kecurian, kerosakan dan gangguan kepada premis dan maklumat.

9.1 Kawalan Kawasan Terhad

Seksyen ini bertujuan untuk menghalang capaian, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat jabatan.

Perkara yang perlu dipatuhi termasuk yang berikut:

- (a) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar, kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemrosesan maklumat;

- (b) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini;
- (c) Merekabentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan;
- (d) Merekabentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, kacau-bilau manusia dan sebarang bencana disebabkan oleh kuasa Tuhan atau perbuatan manusia;
- (e) Melaksanakan perlindungan fizikal dan menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad; dan
- (f) Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari mana-mana pihak yang diberi kebenaran memasukinya.

9.2 Keselamatan Peralatan

Seksyen ini adalah bertujuan untuk mengelak sebarang kehilangan, kerosakan, kecurian atau kompromi (glosari) ke atas aset ICT dan gangguan ke atas sistem penyampaian jabatan.

Perkara yang perlu dipatuhi termasuk yang berikut:

- (a) Perkakasan
 - i. Menempatkan dan mengawal perkakasan-perkakasan ICT supaya risiko ancaman dan bencana dari persekitaran serta percubaan menceroboh oleh pihak yang tidak diberi kebenaran dapat dikurangkan;
 - ii. Semua cadangan perolehan, penempatan dan pengubahsuaian perkakasan-perkakasan ICT hendaklah dirujuk kepada Jawatankuasa Pemanduan ICT JPAM terlebih dahulu; dan
 - iii. Semua cadangan pemindahan perkakasan-perkakasan ICT hendaklah dirujuk kepada Pengurus ICT.
-

(b) Dokumen

Bagi memastikan integriti, kerahsiaan dan kebolehsediaan maklumat serta pengurusan dokumentasi yang baik dan selamat seperti berikut hendaklah dipatuhi:

- i. Memastikan sistem dokumentasi atau penyimpanan maklumat adalah selamat dan terjamin;
- ii. Menggunakan tanda atau label keselamatan seperti Rahsia Besar, Rahsia, Sulit atau Terhad kepada dokumen;
- iii. Satu sistem pengurusan dokumen terperingkat hendaklah diwujudkan bagi menerima, memproses, menyimpan dan menghantar dokumen-dokumen tersebut supaya ianya diuruskan berasingan daripada dokumen-dokumen tidak terperingkat; dan
- iv. Menggunakan penyulitan (enkripsi) ke atas dokumen terperingkat yang disediakan dan dihantar secara elektronik.

(c) Media Storan (Disket, pita magnetik, cakera keras, *CD-ROM*, *optical disk*, *flash disk*, *microfilm* dan lain-lain)

Keselamatan media storan perlu diberi perhatian khusus kerana ia berupaya menyimpan maklumat rasmi dan rahsia rasmi JPAM.

Langkah-langkah pencegahan seperti berikut hendaklah diambil untuk memastikan kerahsiaan, integriti dan kebolehsediaan maklumat yang disimpan dalam media storan adalah terjamin dan selamat:

- i. Menyediakan ruang penyimpanan dan bekas-bekas keselamatan yang mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat;
 - ii. Menghadkan akses kepada pengguna yang dibenarkan sahaja;
 - iii. Sebarang pelupusan hendaklah merujuk kepada tatacara pelupusan; dan
 - iv. Mengadakan sistem pengurusan media termasuk inventori, pergerakan, pelabelan dan *backup/restore*.
-

- (d) Bahan-bahan Habis Guna Terkawal (Kad Mentah Mykad, Mykid, MyPR, iKAd, Buku Pasport, Kad Akses, Sticker Visa dan Pas dan lain-lain)

Keselamatan bahan-bahan habis guna terkawal perlu diberi perhatian khusus kerana ia berupaya menyimpan maklumat rasmi dan rahsia rasmi JPAM.

Langkah-langkah pencegahan seperti berikut hendaklah diambil untuk memastikan kerahsiaan, integriti dan kebolehsediaan maklumat yang disimpan dalam media storan adalah terjamin dan selamat:

- i. Menyediakan ruang penyimpanan dan bekas-bekas keselamatan yang mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat;
- ii. Menghadkan akses kepada pengguna yang dibenarkan sahaja; dan
- iii. Sebarang pelupusan hendaklah merujuk kepada tatacara pelupusan.

9.3 Prasarana Sokongan

- (a) Kawalan Persekitaran

Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk memperoleh dan ubahsuai hendaklah dirujuk terlebih dahulu kepada Pejabat Ketua Pegawai Keselamatan Kerajaan (KPKK). Perkara yang perlu dipatuhi adalah seperti berikut:

- i. Merancang dan menyediakan pelan keseluruhan pusat data termasuk ruang peralatan komputer, ruang percetakan dan ruang atur pejabat;
 - ii. Melengkapi semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan;
-

- iii. Memasang peralatan perlindungan di tempat yang bersesuaian, mudah dikenali dan dikendalikan;
- iv. Menyimpan bahan mudah terbakar di luar kawasan kemudahan penyimpanan aset ICT;
- v. Meletakkan semua bahan cecair di tempat yang bersesuaian dan berjauhan dari aset ICT;
- vi. Dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan ICT; dan
- vii. Menyemak dan menguji semua peralatan perlindungan sekurang-kurangnya dua (2) kali setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu.

(b) Bekalan Kuasa

- i. Melindungi semua peralatan ICT dari kegagalan bekalan elektrik dan menyalurkan bekalan yang sesuai kepada peralatan ICT;
- ii. Menggunakan peralatan sokongan seperti UPS (*Uninterruptable Power Supply*) dan penjana (*generator*) bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan; dan
- iii. Menyemak dan menguji semua peralatan sokongan bekalan kuasa secara berjadual.

(c) Prosedur kecemasan

- i. Memastikan setiap pengguna membaca, memahami dan mematuhi prosedur kecemasan yang ditetapkan oleh Pegawai Keselamatan Jabatan;
 - ii. Melaporkan insiden kecemasan persekitaran seperti kebakaran kepada Pegawai Keselamatan Jabatan;
 - iii. Mengadakan, menguji dan mengemaskini pelan kecemasan
-

dari semasa ke semasa; dan

iv. Mengadakan latihan *fire drill* mengikut jadual.

(d) Keselamatan Kabel

Kabel elektrik dan telekomunikasi yang menyalurkan data atau menyokong sistem penyampaian perkhidmatan hendaklah dilindungi daripada pencerobohan dan kerosakan.

Langkah-langkah keselamatan yang perlu diambil termasuklah seperti berikut:

- i. Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan;
- ii. Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan;
- iii. Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*; dan
- iv. Membuat pelabelan kabel menggunakan kod tertentu.

9.4 Penyelenggaraan Peralatan

Perkakasan hendaklah diselenggarakan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti.

Langkah-langkah keselamatan yang perlu diambil termasuklah seperti berikut:

- (a) Mematuhi spesifikasi yang ditetapkan oleh pengeluar bagi semua perkakasan yang diselenggara;
 - (b) Memastikan perkakasan hanya diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja;
 - (c) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; dan
 - (d) Memaklumkan pihak pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas
-

keperluan.

9.5 Peminjaman Perkasasan Untuk Kegunaan Di Luar Pejabat

Perkakasan yang dipinjam untuk kegunaan di luar pejabat adalah terdedah kepada pelbagai risiko.

Langkah-langkah perlu diambil termasuklah seperti berikut:

- (a) Mendapatkan kelulusan mengikut peraturan yang telah ditetapkan oleh jabatan bagi membawa keluar peralatan, perisian atau maklumat tertakluk kepada tujuan yang dibenarkan;
- (b) Melindungi dan mengawal peralatan sepanjang masa;
- (c) Merekodkan aktiviti peminjaman dan pemulangan peralatan; dan
- (d) Menyemak peralatan yang dipulangkan berada dalam keadaan baik.

9.6 Pengendalian Peralatan Luar Yang Dibawa Masuk/Keluar

Bagi peralatan yang dibawa masuk ke premis JPAM, langkah keselamatan yang perlu diambil adalah seperti berikut:

- (a) Memastikan peralatan yang dibawa masuk tidak mengancam keselamatan ICT JPAM;
- (b) Mendapatkan kelulusan mengikut peraturan yang telah ditetapkan oleh jabatan bagi membawa masuk/keluar peralatan; dan
- (c) Menyemak peralatan yang dibawa keluar tidak mengandungi maklumat JPAM.

9.7 Pelupusan Peralatan

Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan terkini. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan JPAM.

Langkah-langkah hendaklah diambil termasuklah menghapuskan semua

kandungan peralatan khususnya maklumat rahsia rasmi sebelum dilupuskan.

9.8 ***Clear Desk* dan *Clear Screen***

Prosedur *Clear Desk* dan *Clear Screen* perlu dipatuhi supaya maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan.

- (a) Menggunakan kemudahan *password* screen saver atau *logout* apabila meninggalkan komputer;
- (b) Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan
- (c) Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimili dan mesin fotostat.

Bahagian 10: Pengurusan Operasi dan Komunikasi

Penyataan Dasar

Prosedur pengurusan operasi dan komunikasi hendaklah didokumen, dikemaskini dan mudah didapati apabila diperlukan.

Objektif:

Untuk memastikan kemudahan pemprosesan maklumat dan komunikasi adalah berfungsi dengan baik dan selamat dari sebarang ancaman atau gangguan.

10. Pengurusan Operasi Dan Komunikasi

Adalah menjadi tanggungjawab Ketua Jabatan untuk memastikan kesemua kemudahan pemprosesan maklumat adalah terjamin selamat dan berjalan lancar.

10.1 Tanggungjawab Dan Prosedur Operasi

Seksyen ini bertujuan memastikan kemudahan pemprosesan maklumat beroperasi seperti yang ditetapkan.

Perkara yang mesti dipatuhi termasuk yang berikut:

- (a) Semua prosedur operasi hendaklah didokumenkan dengan jelas lagi teratur, dikemaskini dan sedia diguna pakai oleh pengguna mengikut keperluan;
 - (b) Setiap perubahan kepada sistem dan kemudahan pemprosesan
-

maklumat mestilah dikawal;

- (c) Tugas dan tanggungjawab perlu diasingkan bagi mengurangkan risiko kecuiaan dan penyalahgunaan aset jabatan; dan
- (d) Kemudahan ICT untuk pembangunan, pengujian dan operasi mestilah

diasingkan bagi mengurangkan risiko capaian atau pengubahsuaian secara tidak sah kepada sistem yang sedang beroperasi.

10.2 Pengurusan Penyampaian Perkhidmatan Pembekal, Pakar Runding dan Pihak-Pihak Lain Yang Berkepentingan

Seksyen ini bertujuan memastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pembekal, pakar runding dan pihak-pihak lain yang berkepentingan.

Perkara yang mesti dipatuhi termasuk yang berikut:

- (a) Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan diselenggarakan oleh pembekal, pakar runding dan pihak-pihak lain yang berkepentingan;
 - (b) Perkhidmatan, laporan dan rekod yang dikemukakan oleh pembekal, pakar runding dan pihak-pihak lain yang berkepentingan perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa; dan
 - (c) Pengurusan kepada perubahan penyediaan perkhidmatan termasuk menyelenggara dan menambah baik polisi keselamatan, prosedur dan kawalan maklumat sedia ada, perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.
-

10.3 Perancangan Dan Penerimaan Sistem

Seksyen ini bertujuan untuk mengurangkan risiko kegagalan sistem.

Perkara yang mesti dipatuhi termasuk yang berikut:

- (a) Penggunaan peralatan dan sistem mestilah dipantau, ditala (*tuned*) dan perancangan perlu dibuat bagi memenuhi keperluan kapasiti akan datang untuk memastikan prestasi sistem di tahap optimum; dan
- (b) Kriteria penerimaan untuk peralatan dan sistem baru, peningkatan dan versi baru perlu ditetapkan dan ujian yang sesuai ke atasnya perlu dibuat semasa pembangunan dan sebelum penerimaan sistem.

10.4 Perlindungan Dari *Malicious* Dan *Mobile Code*

Seksyen ini bertujuan untuk melindungi integriti maklumat dan perisian dari ancaman *malicious code* seperti *viruses*, *worms*, *trojan horses*, *logic bombs*.

Perkara yang mesti dipatuhi termasuk yang berikut:

- (a) Kawalan pencegahan, pengesanan dan pemulihan untuk melindungi daripada *malicious code*; dan
- (b) Dalam keadaan di mana *mobile code* dibenarkan, konfigurasi hendaklah memastikan bahawa ia beroperasi berdasarkan kepada dasar keselamatan yang jelas dan penggunaan *mobile code* yang tidak dibenarkan adalah dilarang sama sekali.

10.5 Backup

Seksyen ini bertujuan untuk mengekalkan integriti, kesediaan maklumat dan kemudahan pemprosesan maklumat.

Perkara yang mesti dipatuhi termasuk membuat dan menguji secara berkala salinan maklumat dan perisian berdasarkan kepada prosedur *backup*.

10.6 Pengurusan Keselamatan Rangkaian

Seksyen ini bertujuan untuk memastikan perlindungan keselamatan maklumat dalam rangkaian serta infrastruktur sokongan.

Perkara yang mesti dipatuhi termasuk yang berikut:

- (a) Rangkaian perlu dikawal, dipantau dan diurus sebaiknya, bertujuan untuk mengawal daripada sebarang ancaman bagi menjamin keselamatan sistem dan aplikasi yang mengguna rangkaian, termasuk maklumat yang dipindahkan melaluinya; dan
- (b) Ciri-ciri keselamatan, tahap perkhidmatan dan keperluan pengurusan bagi semua perkhidmatan rangkaian perlu dikenal pasti dan dimasukkan dalam mana-mana perjanjian perkhidmatan rangkaian sama ada perkhidmatan berkenaan disediakan secara dalaman atau melalui khidmat luar.

10.7 Pemantauan Rangkaian Berpusat

Seksyen ini bertujuan untuk memastikan pemantauan rangkaian berpusat Kerajaan dapat berfungsi secara berkesan dan berterusan.

JPAM hendaklah memastikan pemantauan dilaksanakan oleh Pemantauan Rangkaian Infrastruktur ICT Sektor Awam Malaysia (PRISMA) ke atas rangkaian JPAM dapat berfungsi secara berkesan dan berterusan.

10.8 Pengendalian Media

Seksyen ini bertujuan untuk memastikan tidak berlaku pendedahan, pengubahsuaian, peralihan atau pemusnahan media secara tidak sah, yang boleh mengganggu aktiviti perkhidmatan.

Perkara yang mesti dipatuhi termasuk yang berikut:

- (a) Prosedur perlu disediakan untuk pengurusan media mudah alih;
 - (b) Media yang tidak digunakan perlu dilupuskan secara selamat mengikut prosedur yang telah ditetapkan;
-

- (c) Prosedur untuk mengendali dan menyimpan maklumat perlu diwujudkan untuk melindungi maklumat daripada didedah tanpa kebenaran atau disalah guna; dan
- (d) Dokumentasi sistem perlu dilindungi dari capaian yang tidak dibenarkan.

10.9 Pertukaran Maklumat

Seksyen ini bertujuan untuk memastikan keselamatan pertukaran maklumat dan perisian dalam jabatan dan mana-mana entiti luar terjamin.

Perkara yang mesti dipatuhi termasuk yang berikut:

- (a) Polisi, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi;
- (b) Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara jabatan dengan pihak luar;
- (c) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dan jabatan;
- (d) Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya; dan
- (e) Polisi dan prosedur perlu dibangunkan dan dilaksanakan bagi melindungi maklumat yang berhubung kait dengan sistem maklumat jabatan.

10.10 Perkhidmatan E-Dagang (transaksi kewangan secara elektronik)

Seksyen ini bertujuan untuk memastikan keselamatan perkhidmatan e-dagang dan penggunaannya.

Perkara yang mesti dipatuhi termasuk yang berikut:

- (a) Maklumat yang terlibat dalam e-dagang perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan
-

pendedahan serta pengubahsuaian yang tidak dibenarkan;

- (b) Maklumat yang terlibat dalam transaksi dalam talian (*on-line*) perlu dilindungi bagi mengelak penghantaran yang tidak salah destinasi, pengubahsuaian, pendedahan, duplikasi atau pengulangan mesej yang tidak dibenarkan; dan
- (c) Integriti maklumat yang disediakan untuk sistem yang boleh dicapai oleh orang awam atau pihak lain yang berkepentingan hendaklah dilindungi untuk mencegah sebarang pindaan yang tidak diperakukan.

10.11 Perkhidmatan Kiosk

Seksyen ini bertujuan untuk memastikan keselamatan perkhidmatan kiosk dan penggunaannya.

Perkara yang mesti dipatuhi termasuk yang berikut:

- (a) Maklumat yang terlibat dalam kiosk perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan;
- (b) Maklumat yang terlibat dalam transaksi dalam talian (*on-line*) perlu dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian, pendedahan, duplikasi atau pengulangan mesej yang tidak dibenarkan; dan
- (c) Integriti maklumat yang disediakan untuk sistem yang boleh dicapai oleh orang awam atau pihak lain yang berkepentingan hendaklah dilindungi untuk mencegah sebarang pindaan yang tidak diperakukan.

10.12 Pemantauan

Seksyen ini bertujuan untuk memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.

Perkara yang mesti dipatuhi termasuk yang berikut:

- (a) Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan
-

disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian;

- (b) Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujudkan dan hasilnya perlu dipantau secara berkala;
 - (c) Kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan;
 - (d) Aktiviti pentadbiran dan operator sistem perlu direkodkan;
 - (e) Kesalahan, kesilapan dan/atau penyalahgunaan perlu dilog, dianalisis dan diambil tindakan sewajarnya; dan
 - (f) Masa yang berkaitan dengan sistem pemprosesan maklumat dalam organisasi atau domain keselamatan perlu diselaraskan dengan satu sumber masa yang dipersetujui.
-

Bahagian 11: Kawalan Capaian

Penyataan Dasar:

Capaian ke atas maklumat, kemudahan pemprosesan maklumat dan proses-proses utama dalam teras perkhidmatan perlu dikawal mengikut ketetapan yang ditentukan oleh pengurusan, pemilik data, proses, operasi atau sistem.

Objektif:

Untuk mengawal capaian ke atas maklumat.

11. Pengurusan Kawalan Capaian

Adalah menjadi tanggungjawab Ketua Jabatan untuk memastikan kawalan capaian ke aset ICT termasuk maklumat, perkhidmatan rangkaian dan kemudahan yang berkaitan diwujudkan dan dilaksanakan dengan berkesan berasaskan keperluan perkhidmatan dan keselamatan.

11.1 Keperluan Kawalan Capaian

Seksyen ini bertujuan mengawal capaian ke atas maklumat, kemudahan proses maklumat, dan proses perkhidmatan berdasarkan keperluan perkhidmatan dan keperluan keselamatan. Peraturan kawalan capaian hendaklah mengambil kira penyebaran dan pengesahan maklumat.

Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan.

Perkara yang perlu dipastikan termasuk seperti berikut:

- (a) Kawalan capaian ke atas maklumat dan proses perkhidmatan
-

- mengikut keperluan keselamatan dan peranan pengguna;
- (b) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran;
 - (c) Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; dan
 - (d) Kawalan ke atas kemudahan pemrosesan maklumat.

11.2 Pengurusan Capaian Pengguna

Seksyen ini bertujuan memastikan bahawa sistem maklumat dicapai oleh pengguna yang sah dan menghalang capaian yang tidak sah.

Perkara yang perlu dipatuhi adalah termasuk :

- (a) Mewujudkan prosedur pendaftaran dan pembatalan kebenaran kepada pengguna untuk mencapai maklumat dan perkhidmatan;
 - (b) Akaun pengguna adalah unik dan pengguna bertanggungjawab ke atas akaun tersebut selepas pengesahan penerimaan dibuat;
 - (c) Akaun pengguna yang diwujudkan dan tahap capaian termasuk sebarang perubahan mestilah mendapat kebenaran ketua jabatan secara bertulis dan direkodkan;
 - (d) Pemilikan akaun dan capaian pengguna adalah tertakluk kepada peraturan jabatan dan tindakan pengemaskinian dan/atau pembatalan hendaklah diambil atas sebab seperti berikut:
 - i. Pengguna tidak hadir bertugas tanpa kebenaran melebihi satu tempoh yang ditentukan oleh ketua jabatan;
 - ii. Pengguna bercuti atau bertugas di luar pejabat dalam satu tempoh yang lama seperti mana yang ditentukan oleh Ketua Jabatan;
 - iii. Pengguna bertukarjawatan, tanggungjawab dan/atau bidang tugas;
 - iv. Pengguna yang sedang dalam prosiding dan/atau
-

dikenakan tindakan tatatertib oleh Pihak Berkuasa Tatatertib; dan

- v. Pengguna bertukar, berpindah jabatan, bersara dan/atau tamat perkhidmatan.
- (e) Aktiviti capaian oleh pengguna direkod, diselenggara dengan sistematik dan dikaji dari masa ke semasa. Maklumat yang direkod termasuk identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh, masa, rangkaian dilalui, aplikasi diguna dan aktiviti capaian secara sah atau sebaliknya.

11.3 Tanggungjawab Pengguna

Seksyen ini bertujuan memastikan pengguna melaksanakan langkah berkesan ke atas kawalan capaian untuk menghalang penyalahgunaan, kecurian maklumat dan kemudahan proses maklumat.

Perkara yang perlu dipatuhi adalah termasuk yang berikut:

- (a) Mematuhi amalan terbaik pemilihan dan penggunaan kata laluan;
- (b) Memastikan kemudahan dan peralatan yang tidak digunakan mendapat perlindungan sewajarnya; dan
- (c) Mematuhi amalan *clear desk policy* atau *clear screen policy*.

11.4 Kawalan Capaian Rangkaian

Seksyen ini bertujuan menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian. Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan:

- (a) Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian organisasi, rangkaian organisasi lain dan rangkaian awam;
 - (b) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan, yang menepati kesesuaian penggunaannya; dan
-

- (c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.

11.5 Kawalan Capaian Sistem Pengoperasian

Seksyen ini bertujuan memastikan bahawa capaian ke atas sistem pengoperasian dikawal dan dihadkan kepada pengguna yang dibenarkan sahaja. Kaedah yang digunakan hendaklah mampu menyokong perkara berikut:

- Mengesahkan pengguna yang dibenarkan selaras dengan peraturan organisasi;
- Mewujudkan *audit trail* ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf *super user*;
- Menjana amaran (*alert*) sekiranya berlaku pelanggaran ke atas peraturan keselamatan sistem;
- Menyedia kaedah sesuai untuk pengesahan capaian (*authentication*); dan
- Menghadkan tempoh penggunaan mengikut kesesuaian. Perkara yang perlu dipatuhi termasuk yang berikut:
 - (a) Mengawal capaian ke atas sistem operasi menggunakan prosedur *log-on* yang terjamin;
 - (b) Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja dan satu teknik pengesahan yang bersesuaian hendaklah diwujudkan bagi mengesahkan pengenalan diri pengguna;
 - (c) Mewujudkan sistem pengurusan kata laluan secara interaktif dan memastikan kata laluan adalah berkualiti;
 - (d) Menghadkan dan mengawal penggunaan program utiliti yang berkemampuan mengatasi sebarang kawalan sistem dan aplikasi;
 - (e) Menamatkan sesebuah sesi yang tidak aktif sekiranya tidak digunakan bagi satu tempoh yang ditetapkan; dan

- (f) Menghadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.

11.6 Kawalan Capaian Rangkaian

Seksyen ini bertujuan menghalang capaian tidak sah ke atas maklumat yang terdapat di dalam sistem aplikasi. Kawalan capaian hendaklah:

- Membenarkan pengguna mencapai aplikasi dan maklumat mengikut tahap capaian yang ditentukan;
- Menyediakan mekanisme perlindungan bagi menghalang capaian tidak sah ke atas aplikasi dan maklumat daripada utiliti yang sedia ada dalam sistem operasi dan perisian *malicious* yang berupaya melangkaui kawalan sistem; dan
- Tidak berkompromi dengan sebarang sistem yang berkongsi sumber.

Perkara yang perlu dipatuhi termasuk yang berikut:

- (a) Menghadkan capaian ke atas maklumat dan fungsi sistem aplikasi oleh pengguna selaras dengan peraturan organisasi; dan
- (b) Mewujudkan persekitaran pengkomputeran yang khusus dan terasing untuk sistem yang berklasifikasi tinggi.

11.7 Peralatan Mudah Alih Dan Kerja Jarak Jauh

Seksyen ini bertujuan memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan kerja jarak jauh.

Perkara yang perlu dipatuhi termasuk yang berikut:

- (a) Mewujudkan peraturan dan garis panduan keselamatan yang bersesuaian untuk melindungi dari risiko penggunaan peralatan mudah alih dan kemudahan komunikasi; dan
 - (b) Mewujudkan peraturan dan garis panduan untuk memastikan persekitaran kerja jarak jauh adalah sesuai dan selamat.
-

Bahagian 12: Perolehan, Pembangunan dan Penyelenggara Sistem Maklumat

Penyataan Dasar:

Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem maklumat sedia ada atau sistem maklumat baru hendaklah menyatakan keperluan-keperluan kawalan keselamatan.

Objektif:

Untuk memastikan aspek keselamatan dikenal pasti dan diambil kira dalam semua sistem maklumat dan/atau perkhidmatan termasuk sistem pengoperasian, infrastruktur, sistem aplikasi dan sistem perisian. Aspek keselamatan ini mesti dikenal pasti, dijustifikasikan, dipersetujui dan didokumentasikan sebelum sesuatu sistem maklumat direka bentuk dan dilaksanakan.

12. Perolehan, Pembangunan dan Penyelenggaraan Sistem Maklumat Tanggungjawab Ketua Jabatan adalah untuk:

- (a) Memastikan kaedah keselamatan yang bersesuaian dikenal pasti, dirancang dan dilaksanakan pada setiap peringkat perolehan, pembangunan dan penyelenggaraan sistem maklumat;
 - (b) Melindungi kerahsiaan, integriti dan kesahihan maklumat menggunakan kaedah tertentu;
 - (c) Memastikan sistem fail dan aktiviti berkaitan beroperasi dengan baik dan selamat; dan
 - (d) Menjaga dan menjamin keselamatan sistem maklumat.
-

12.1 Keperluan Keselamatan Sistem Maklumat

Seksyen ini bertujuan menjelaskan keperluan memastikan bahawa aspek keselamatan dikenal pasti, dipersetujui dan didokumen pada setiap peringkat perolehan, pembangunan dan penyelenggaraan.

Perkara yang perlu dipatuhi adalah termasuk yang berikut:

- (a) Pernyataan keperluan bagi sistem maklumat baru atau penambahbaikan ke atas sistem sedia ada hendaklah menjelaskan mengenai kawalan jaminan keselamatan.

12.2 Pemprosesan Aplikasi Dengan Tepat

Seksyen ini bertujuan memastikan kawalan keselamatan yang sesuai digarap dan dijalin ke dalam aplikasi bagi menghalang kesilapan, kehilangan, pindaan yang tidak sah dan penyalahgunaan maklumat dalam aplikasi.

Perkara yang perlu dipatuhi adalah termasuk yang berikut:

- (a) Menyemak dan mengesahkan input data sebelum dimasukkan ke dalam aplikasi bagi menjamin kesahihan dan ketepatan;
- (b) Menggabungkan semakan pengesahan ke dalam aplikasi untuk mengenal pasti sebarang kerosakan maklumat sama ada disebabkan oleh ralat pemprosesan atau tindakan yang disengajakan;
- (c) Mengetahui dan melaksanakan kawalan untuk mengesah dan melindungi integriti mesej dalam sistem aplikasi; dan
- (d) Melaksanakan proses pengesahan ke atas output data bagi menjamin kesahihan dan ketepatan pemprosesan sistem aplikasi.

12.3 Kawalan Kriptografi

Seksyen ini bertujuan untuk melindungi kerahsiaan, kesahihan dan integriti maklumat melalui teknik kriptografi.

Perkara yang perlu dipatuhi adalah termasuk membangun kawalan

kegunaan dan melaksanakan suatu peraturan kawalan kriptografi dan pengurusan kunci yang digunakan untuk menyokong teknik kriptografi bagi melindungi maklumat.

12.4 Keselamatan Fail-fail Sistem

Seksyen ini bertujuan memastikan capaian ke atas fail-fail sistem dan kod sumber program adalah terkawal dan aktiviti-aktiviti sokongan dilaksanakan dalam kaedah yang selamat. Kawalan perlu diambil untuk mengelakkan pendedahan maklumat sensitif semasa proses pengujian dilaksanakan.

Perkara yang perlu dipatuhi adalah termasuk yang berikut:

- (a) Mewujudkan peraturan untuk mengawal pemasangan perisian ke dalam sistem yang sedang beroperasi;
- (b) Melindungi dan mengawal data-data ujian; dan
- (c) Menghadkan capaian ke atas kod sumber program.

12.5 Keselamatan Dalam Proses Pembangunan Dan Sokongan

Seksyen ini bertujuan memastikan keselamatan perisian sistem aplikasi dan maklumat dikawal supaya selamat dalam semua keadaan.

Perkara yang perlu dipatuhi adalah termasuk yang berikut:

- (a) Mengawal pelaksanaan perubahan menggunakan prosedur kawalan perubahan yang formal;
 - (b) Mengkaji semula dan menguji aplikasi kritikal semasa melaksanakan perubahan ke atas sistem yang sedang beroperasi untuk memastikan tiada impak negatif ke atas keselamatan atau operasi organisasi;
 - (c) Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja;
 - (d) Menghalang sebarang peluang untuk membocorkan maklumat;
-

- (e) Mengawal selia dan memantau pembangunan perisian oleh pembekal, pakar runding dan pihak-pihak lain yang berkepentingan.

12.6 Pengurusan Teknikal *Vulnerability*

Seksyen ini bertujuan memastikan pelaksanaan pengurusan teknikal *vulnerability* adalah berkesan, sistematik dan berkala dengan mengambil langkah-langkah yang bersesuaian untuk menjamin keberkesanannya. Pelaksanaan pengurusan teknikal *vulnerability* ini perlu juga dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara yang perlu dipatuhi adalah termasuk memperoleh maklumat teknikal *vulnerability* yang tepat pada masanya ke atas sistem maklumat yang digunakan, menilai tahap pendedahan organisasi terhadap *vulnerability* tersebut dan mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.

Bahagian 13: Pengurusan Pengendalian Insiden Keselamatan

Penyataan Dasar:

Semua insiden keselamatan ICT yang berlaku di jabatan-jabatan Kerajaan mestilah dilaporkan dengan serta-merta dan dikendalikan mengikut peraturan atau prosedur pengurusan pengendalian insiden keselamatan ICT Kerajaan yang ditetapkan.

Objektif :

Untuk memastikan semua insiden dikendalikan dengan cepat, tepat dan berkesan, dan memastikan sistem ICT Kerajaan dapat segera beroperasi semula dengan baik supaya tidak menjejaskan imej jabatan dan sistem penyampaian perkhidmatan awam.

13. Pengurusan Pengendalian Insiden Keselamatan

Ketua Jabatan adalah bertanggungjawab untuk memastikan jabatan-jabatan di bawah kawalannya mematuhi arahan mengenai pengurusan pengendalian insiden keselamatan ICT di jabatan masing-masing dengan merujuk kepada pekeliling am, surat pekeliling am, garis panduan dan prosedur operasi standard yang telah dikeluarkan oleh Kerajaan.

13.1 Insiden Keselamatan

Insiden keselamatan ICT bermaksud musibah (*adverse event*) yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar dasar keselamatan ICT sama ada yang ditetapkan secara tersurat atau tersirat.

Ketua Jabatan hendaklah melaksanakan tindakan ke atas insiden keselamatan ICT mengikut peraturan atau prosedur yang ditetapkan oleh Kerajaan dari semasa ke semasa.

13.2 Mekanisme Pelaporan Insiden Keselamatan ICT

(a) Pelaporan

Semua insiden keselamatan ICT yang berlaku mesti dilaporkan kepada Pegawai Keselamatan ICT (ICTSO) jabatan dan kepada Jabatan Pertahanan Awam Malaysia *Computer Emergency Response Team* (JPAM CERT), Kementerian Dalam Negeri *Computer Emergency Response Team* (KDN CERT) atau kepada *Government Computer Emergency Response Team* (GCERT), untuk pengendalian dan pengumpulan statistik insiden keselamatan ICT Kerajaan. Semua maklumat adalah SULIT, dan hanya boleh didedahkan kepada pihak-pihak yang dibenarkan.

(b) Pelantikan Pegawai Bertanggungjawab

Pegawai Keselamatan ICT jabatan dan anggota pasukan CERT jabatan mestilah dilantik secara rasmi oleh pengurusan jabatan masing-masing, dan semua warga jabatan berkenaan perlu maklum akan pelantikan pegawai-pegawai ini, dan perlu sentiasa bersedia untuk memberi respon apabila diperlukan.

(c) Tanggungjawab Pengguna

Semua penjawat awam, pembekal, pakar runding dan pihak-pihak lain yang terlibat diingatkan supaya tidak melaksanakan sebarang tindakan secara sendiri, tapi sebaliknya perlu terus melaporkan dengan segera sebarang kejadian insiden keselamatan ICT, kerentanan yang diperhatikan atau disyaki terdapat dalam perkhidmatan dan sistem maklumat jabatan menerusi mekanisme pelaporan ini. Ini adalah bagi mengelakkan kerosakan atau kehilangan bahan bukti pencerobohan dan cubaan pencerobohan.

(d) Tindakan Dalam Keadaan Berisiko Tinggi

Dalam keadaan atau persekitaran berisiko tinggi, pengurusan

atasan hendaklah dimaklumkan dengan serta-merta supaya satu keputusan segera dapat diambil. Tindakan ini perlu bagi mengelakkan kesan atau impak kerosakan yang lebih teruk dan mengelakkan kejadian insiden merebak kepada jabatan-jabatan.

13.3 Prosedur Pengendalian Insiden Keselamatan ICT

Semua pegawai pasukan pengendali insiden keselamatan ICT iaitu anggota JPAM CERT perlu melaksanakan pengurusan pengendalian insiden keselamatan ICT berpandukan prosedur operasi standard keselamatan ICT GCERT dan KDN CERT.

13.4 Pengurusan Maklumat Insiden Keselamatan ICT

(a) Perancangan

Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan dan dianalisis bagi tujuan perancangan dan tindakan untuk melaksanakan peningkatan dan kawalan tambahan bagi mengawal kekerapan, kerosakan dan kos kejadian insiden akan datang, dan untuk tujuan mengkaji semula dasar-dasar keselamatan aset ICT sedia ada. Maklumat ini juga digunakan untuk mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada jabatan.

(b) Bahan Bukti

Jabatan hendaklah memastikan bahan-bahan bukti berkaitan insiden keselamatan ICT dapat disediakan, disimpan, diselenggarakan dan mempunyai perlindungan keselamatan. Penyediaan bahan-bahan bukti seperti jejak audit, *backup* secara berkala, media *backup offline* ini hendaklah mengikut amalan terbaik yang disarankan oleh kerajaan dari semasa ke semasa.

Jabatan juga hendaklah memastikan semua bahan bukti adalah selaras dengan peraturan pengumpulan maklumat dari segi kualiti, kelengkapan dan kebolehpercayaan bahan bukti yang termaktub dalam bidang kuasa perundangan berkenaan.

Perkara-perkara yang mesti dipatuhi termasuk yang berikut:

- i. Melindungi integriti semua bahan bukti;
 - ii. Menjalinkan bahan bukti oleh personel yang
-

dipertanggungjawabkan;

- iii. Merekod semua maklumat aktiviti penyalinan termasuk pegawai terlibat, media, perisian, perkakasan dan *tools* yang digunakan;
 - iv. Memaklumkan pihak berkuasa perundangan, seperti pegawai undang-undang dan polis (jika perlu); dan
 - v. Mendapatkan nasihat dari pihak berkuasa perundangan ke atas bahan bukti yang perlukan.
-

Bahagian 14: Pengurus Kesenambungan Perkhidmatan

Penyataan Dasar:

Pengurusan kesinambungan perkhidmatan dan pelan pengurusan kesinambungan perkhidmatan hendaklah diwujudkan dan dilaksanakan berdasarkan kepada persekitaran dan operasi jabatan.

Objektif:

Untuk memastikan penyampaian perkhidmatan yang berterusan kepada pelanggan.

14. Pengurus Kesenambungan Perkhidmatan

Pengurusan Kesenambungan Perkhidmatan adalah mekanisme bagi mengurus dan memastikan kepentingan *stakeholder* sistem penyampaian perkhidmatan dilindungi dan imej jabatan terpelihara dengan mengenal pasti kesan atau impak yang berpotensi menjejaskan sistem penyampaian perkhidmatan jabatan di samping menyediakan pelan tindakan bagi mewujudkan ketahanan dan keupayaan bertindak yang berkesan.

Ketua Jabatan adalah bertanggungjawab untuk memastikan operasi sistem penyampaian perkhidmatan di bawah kawalannya disediakan secara berterusan tanpa gangguan di samping menyediakan perlindungan keselamatan kepada aset ICT jabatan.

14.1 Pelan Kesenambungan Perkhidmatan

Pelan Kesenambungan Perkhidmatan hendaklah dibangunkan bagi menentukan pendekatan yang menyeluruh diambil mengekalkan kesinambungan perkhidmatan jabatan. Ini bertujuan memastikan tindakan pemulihan yang cekap dan berkesan dilaksanakan apabila berlakunya musibah atau bencana.

Perkara-perkara berikut yang mesti dipatuhi termasuk berikut:

(a) Perakuan Pengurusan

Pelan ini mestilah diperakukan oleh pengurusan jabatan.

(b) Program Latihan/Kesedaran

Program latihan/kesedaran kepada semua warga jabatan mengenai pelan ini dan proses serta prosedur yang terlibat perlu dilaksanakan.

(c) Penyelenggaraan Pelan

Pelan Kesenambungan Perkhidmatan perlu diselenggara secara berkala dan diuji pelaksanaannya terutama apabila terdapat perubahan dalam operasi dan sistem penyampaian perkhidmatan jabatan/Kerajaan.

Bahagian 15: Pematuhan

Penyataan Dasar:

Keperluan-keperluan perundangan, *statutory*, peraturan atau ikatan kontrak hendaklah dinyatakan, didokumenkan dan dikemaskini.

Objektif:

Untuk menghindar pelanggaran undang-undang jenayah dan sivil, *statutory*, peraturan atau ikatan kontrak dan sebarang keperluan keselamatan lain.

15. Pematuhan Keperluan Perundangan

Adalah menjadi tanggungjawab Ketua Jabatan untuk memastikan bahawa pematuhan dan sebarang pelanggaran dielakkan.

15.1 Pematuhan Dasar

Langkah-langkah perlu bagi mengelakkan sebarang pelanggaran perundangan termasuklah memastikan setiap pengguna membaca, memahami dan mematuhi Dasar Keselamatan ICT JPAM dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa.

15.2 Keperluan Perundangan

Keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di jabatan termasuklah seperti berikut:

- (a) Keselamatan perlindungan secara am
- i. *Emergency (Essential Power) Act 1964*;
 - ii. *Essential (Key Points) regulations 1965*;
 - iii. Arahan Keselamatan Yang Dikuatkuasakan Melalui Surat Pekeliling Am Sulit Bil. 1 Tahun 1985;
 - iv. Arahan Jawatankuasa Tetap Sasaran Penting Bil. 1 Tahun 1985;
 - v. Arahan Tetap Sasaran Penting Yang Dikeluarkan Kepada Pihak Yang Terlibat Dalam Pengurusan Sasaran Penting Milik Kerajaan Dan Swasta Yang Diluluskan Oleh Jemaah Menteri Pada 13 Oktober 1993; dan
- (b) Keselamatan Dokumen
- i. *Confidential General Circular Memorandum No.1 of 1959 (Code Words-Allocation & Control)*;
 - ii. Akta Rahsia Rasmi 1972;
 - iii. Akta Arkib Negara 2003;
 - iv. Surat Pekeliling Bil. 8 Tahun 1990 - Arahan Keselamatan Kawalan, Penyelenggaraan, Maklumat-Maklumat Ukur Dan Geografi Yang Antara Lainnya Merangkumi Peta-Peta Rasmi Dan Penderiaan Jauh;
 - v. Surat Pekeliling Am Sulit Bil. 1 Tahun 1972 - Keselamatan Rahsia-Rahsia Kerajaan Daripada Ancaman Penyuluhan (*espionage*);
 - vi. Surat Pekeliling Am Bil. 2 Tahun 1987 - Peraturan Pengurusan Rahsia Rasmi Selaras Dengan Peruntukan-Peruntukan Akta Rahsia Rasmi (Pindaan) 1976;
 - vii. Peraturan Pengurusan Rahsia Rasmi Selaras dengan Peruntukan-Peruntukan Akta Rahsia Rasmi (Pindaan)
-

1986 Dan Surat Pekeliling Am Bil. 2 Tahun 1987 Yang Ditandatangani Oleh Y.Bhg Ketua Setiausaha Negara Melalui Surat M(R)10308/3/(45) Bertarikh 8 Mei 1987; dan

- viii. Kawalan Keselamatan Rahsia Rasmi Dan Dokumen Rasmi Kerajaan Yang Dikelilingkan melalui Surat KPKK(R)200/55 Klt.7(21) Bertarikh 21 Ogos 1999.

(c) Keselamatan Fizikal Bangunan

- i. Akta Kawasan Larangan Dan Tempat Larangan Tahun 1959;
- ii. Arahan Pembinaan Bangunan Berdekatan Dengan Sasaran Penting, Kawasan Larangan Dan Tempat Larangan;
- iii. *State Key Points*;
- iv. Surat Pekeliling Am Rahsia Bil. 1 Tahun 1975 - Keselamatan Jabatan-Jabatan Kerajaan;
- v. Surat Bil. KPKK/308/A (2) bertarikh 7/9/79 - Mencetak Pas-Pas Keselamatan dan Kad-Kad Pengenalan Kementerian/ Jabatan;
- vi. Surat pekeliiling Am Bil. 4 tahun 1982 – Permohonan Ruang Pejabat Sama Ada Dalam Bangunan Guna sama Atau pun Disewa Di Bangunan Swasta; dan
- vii. Surat Pekeliling Am Bil. 14 Tahun 1982 – Pelaksanaan Pelan Pejabat Terbuka.

(d) Keselamatan Individu

- i. *Government Security Officer: Terms of Reference - Extract On Training of Departmental Security Office Confidential*;
 - ii. *General Circular Memorandum*;
 - iii. *Instruction On Positive Vetting Procedure*;
 - iv. Surat Pekeliling Am Sulit Bil. 1/1966 - Perkara Keselamatan
-

Tentang Persidangan-Persidangan/Perjumpaan Lawatan Sambil Belajar Antarabangsa;

- v. Surat Pekeliling Tahun 1966 - Tapisan Keselamatan Terhadap Pakar/Penasihat Luar Negeri;
- vi. Surat Pekeliling Am Sulit Bil. 1/1967 - Ceramah Keselamatan bagi Pegawai-Pegawai Kerajaan dan mereka-mereka yang Bukan Pegawai-Pegawai Kerajaan yang bersama dalam Perwakilan Rasmi Malaysia semasa melawat Negara-negara Tabir Buluh dan Tabir Besi;
- vii. Surat Pekeliling Am Sulit Bil. 2 Tahun 1977 - Melaporkan Perjumpaan/ Percakapan Di Antara Diplomat/Orang-Orang Perseorangan Dari Negeri-Negeri Asing Dengan Anggota-Anggota Kerajaan; dan
- viii. Pekeliling Kemajuan Pentadbiran Awam Bil. 1 Tahun 2003 Garis Panduan mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Jabatan-Jabatan Kerajaan.

(e) Keselamatan Aset ICT

- i. Akta Tandatangan Digital 1997;
 - ii. Akta Jenayah Komputer 1997;
 - iii. Akta Hak Cipta (Pindaan) 1997;
 - iv. Akta Multimedia dan Telekomunikasi 1998;
 - v. Surat Pekeliling Am Bil. 1 Tahun 1993 - Peraturan Penggunaan Mesin Faksimile di Pejabat-Pejabat Kerajaan;
 - vi. Pekeliling Am Bil. 3 Tahun 2000 - Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi;
 - vii. Pekeliling Am Bil. 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat & Komunikasi (ICT);
 - viii. Pekeliling Kemajuan Pentadbiran Awam Bil. 1 Tahun 2003 - Garis Panduan Mengenai Tatacara Penggunaan Internet & Mel Elektronik di Jabatan-Jabatan Kerajaan;
-

- ix. *Malaysian Public Sector Management of Information & Communication Technology Security Handbook (MyMIS) 2002*; dan
 - x. Surat Pekeliling Am Bilangan 6 Tahun 2005 - Garis Panduan Melaksanakan Penilaian Risiko Keselamatan Maklumat Sektor Awam bertarikh 7 November 2005.
- (f) Akta-akta dan Peraturan-peraturan lain yang berkaitan dengan JPAM;
- i. Akta 221
 - Akta Pertahanan Awam 1951 (Disemak 1979)
 - Kaedah-kaedah Pertahanan Awam (Bencana Diri) 1970
 - Kaedah-kaedah Pertahanan Awam (Pasukan Pertahanan Awam) 1970
 - Peraturan Pertahanan Awam (Pakai Seragam) 1983
 - ii. Akta 425
 - Akta Perkhidmatan Negara 1952 (Semakan 1990)
 - Perlembagaan Malaysia - Jadual Kesembilan
 - Skim 'Non-Operational' Pertahanan Awam
 - Pelan Kontinjensi Kebangsaan Menghadapi Peperangan
 - Dasar Pertahanan Menyeluruh (HANRUH)
 - Arahan Menteri
 - Arahan Dan Pekeliling Jabatan
 - Deklarasi ICDO (*International Civil Defence Organisation*)
 - iii. Arahan MKN (Majlis Keselamatan Negara)
 - Arahan No.18
 - Arahan No.20
 - Arahan No.21
-

15.3 Pelanggaran Perundangan

Mengambil tindakan undang-undang dan tatatertib ke atas sesiapa yang terlibat di dalam semua perbuatan kecuaiian, kelalaian dan pelanggaran keselamatan yang membahayakan perkara-perkara terperingkat di bawah Akta Rahsia Rasmi 1972 dan akta-akta dan peraturan-peraturan lain yang berkaitan.